UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,487	08/16/2001	Edward W. Kohler JR.	12221-006001	3664

26161 7590 07/05/2007
FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
ISMAIL, SHAWKI SAIF	
ART UNIT	**PAPER NUMBER**
2155	
MAIL DATE	**DELIVERY MODE**
07/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/931,487
Filing Date: August 16, 2001
Appellant(s): KOHLER ET AL.

Mazu Networks, Inc.
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed March 14, 2007 appealing from the Office action mailed June 14, 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Method and system for diagnosing network intrusion by Yavatkar et al U.S. Patent No. 6,735702

Adaptive system and method for responding to computer network security attacks by Hill et al U.S. Patent No. 6,088,804

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC §102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Claims 1-12 and 15-33 are rejected under 35 U.S.C. 102(e) as being anticipated by **Yavatkar et al.,** (Yavatkar) U.S. Patent No. **6,735,702.**

As to claim 1, Yavatkar teaches a method of protecting a data center against a denial of service attack, the method comprises:

sending queries to data collectors, deployed at different points in a network that carries network traffic to the data center, the data collectors collect statistical information on network packets sent over the network, the queries to request the statistical information from at least some of the data collectors (col. 3 line 65 – col. 4, line 23, launching of the various types of bloodhound agents);

sending the statistical information from the data collectors in response to the queries (col. 3 line 65 – col. 4, line 23, bloodhound agents gather data and report back to the watchdog agents);

processing the statistical information to determine the source of suspicious network traffic heir sent to the data center (col. 3, lines 25-37 and col. 18, lines 32-53, agents are deployed at different areas of the network for the detection and diagnosing of various network attacks as well as for collecting statistical information on a particular node).

As to claim 2, Yavatkar teaches the method of claim 1 wherein the network packets from the attacker have faked, random source addresses that change with time, and sending queries further comprises:

sending queries to the data collectors for the statistical information based on victim destination address (col. 13, lines 44-53 and col. 3, line 65 – col. 4, line 23, the agents are deployed to specific areas of the network depending on the source of the attack).

As to claim 3, Yavatkar teaches the method of claim 1 wherein processing further comprises:

Determining, from at least in part, the collected statistical information, what data centers are involved in the attack on the victim data center (col. 8, lines 32-53, the agents determine the source of the attack and other nodes that it affected).

As to claim 4, Yavatkar teaches the method of claim 3 wherein determining is performed by a control center that receives the statistical information from the data collectors, and determining further comprises:

sending data to/from a gateway device that is associated with the victim data center (col. 13 line 54 – col. 14, line 17, the gateway associated with the attack is identified and measures are taken to filter the attack).

As to claim 5, Yavatkar teaches the method of claim 4 wherein the gateway identifies the network address of the victim, via a message to the control center (col. 13 line 54 – col. 14, line 17).

As to claim 6, Yavatkar teaches the method of claim 5 wherein the queries and the statistical information are sent over a redundant network that does not carry the packet traffic to deliver collected statistical information to a central control enter in response to the queries sent from the central control center (see Fig. 3).

As to claim 7, Yavatkar teaches the method of claim 5 wherein message indicates the type of attack (col. 3, lines 35-45 and col. 4, lines 41-61).

As to claim 8, Yavatkar teaches the method of claim 1 wherein a source of the attack is behind a gateway (col. 13 line 54 – col. 14, line 17)

As to claim 9, Yavatkar teaches the method of claim 8 wherein if a source of the attack is behind a gateway, the control center issues a request to the gateway that the attacking system is behind to prevent the attacking traffic from attacking system from reaching the network (col. 13 line 54 – col. 14, line 17).

As to claim 10, Yavatkar teaches the method of claim 8 wherein if a source of the attack is behind a gateway, the gateway that the attacking system is behind selectively discards traffic that appears to be malicious traffic and that contains the victim destination address (col. 13 line 54 – col. 14, line 17).

As to claim 11, Yavatkar teaches the method of claim 1 wherein if source of the attack is not behind a gateway, the control center queries the data collectors to provide information about possible locations of the attacking system (col. 13 line 54 – col. 14, line 17).

As to claim 12, Yavatkar teaches the method of claim 1 wherein if source of the attack is not behind a gateway, the method further comprises:

contacting administrators at locations involved in the attack to have the administrators take action to filter out packets with the destination address (col. 13 line 54 – col. 14, line 17, and col. 18, line 54 – col. 19, line 6).

As to claim 15, Yavatkar teaches a method of protecting a victim data center against a denial of service attack, the method comprises:

receiving packets with faked, random source addresses (col. 13, lines 44-53);

receiving, from a gateway disposed near the victim data center, a notification that the victim data center is under an attack (col. 13 line 54 – col. 14, line 17, and col. 18, line 54 – col. 19, line 6);

sending queries to data collectors deployed at different points in a network that carries network traffic to the victim data center, the data collectors to sample network packets and collect statistical information on network packets sent over the network the

queries being request for statistical information from data collectors that have examined network traffic with the victim destination address (col. 3, lines 25-37 and col. 18, lines 32-53); and

determining the data center or centers involved in the attack on the victim data center by analyzing collected statistical information from the data collectors (col. 18, lines 32-53).

As to claim 16, Yavatkar teaches the method of claim 15 further comprising:

Communicating statistical information from the control center to/from a gateway device that is disposed with the victim data center (col. 13 line 54 – col. 14, line 17).

As to claim 17, Yavatkar teaches the method of claim 16 wherein if a source of the attack is behind a gateway, the control center issues a request to the gateway to block the attacking traffic (col. 13 line 54 – col. 14, line 17).

As to claim 18, Yavatkar teaches the method of claim 17 wherein if a source of the attack is behind a gateway, the gateway selectively discards traffic that appears to be malicious traffic and that contains the victim destination address (col. 13 line 54 – col. 14, line 17).

As to claim 19, Yavatkar teaches the method of claim 15 wherein if a source of the attack is not behind a gateway, the method comprises:

contacting administrators at locations involved in attack to filter out packets having the destination address (col. 13 line 54 – col. 14, line 17, and col. 18, line 54 – col. 19, line 6).

As to claim 20, Yavatkar teaches a system to thwart denial of service attacks on a victim data center, the system comprising:

a plurality of monitors dispersed throughout a network, the monitors collecting statistical data on network traffic (col. 3, lines 25-37 and col. 18, lines 32-53);

a control center coupled to the plurality of data collectors, the control center executing a computer program product stored on a computer readable medium, comprising instructions for causing a computer to:

receive from the victim site a notification that the victim data center is under an attack (col. 13 line 54 – col. 14, line 17, and col. 18, line 54 – col. 19, line 6); and in response to receiving the notification,

send queries to data collectors to request the statistical information from the data collectors, the statistical information used to determine the source of suspicious network traffic being sent to the victim (col. 3, lines 25-37 and col. 18, lines 32-53);

a gateway device that passes network packets between the network and the victim data center, the gateway disposed to protect the victim data center, and being coupled to the control center (col. 13 line 54 – col. 14, line 17).

Claims 21-33 do not teach or define any new limitation beyond claims 1-20 above, therefore, they are rejected for similar reasons.

Claim Rejections - 35 USC §103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject

> matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 13 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Yavatkar et al.,** (Yavatkar) U.S Patent No. **6,735,702** and in view of **Hill et al.,** (Hill) U.S. Patent No. **6,088,804.**

As to claim 13 and 14, Yavatkar teaches a method for blocking denial of service and address spoofing attacks on a network. However, Yavatkar does not explicitly teach wherein the attacks are classified into categories based on the severity that they cause to the network.

Hill teaches a system and method for adaptively responding to computer network security attacks. Hill further teaches classifying attacks based on the severity of the attack on the network (Fig. 3, col. 2; lines 53-60; col. 6, lines 9-22).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate Hill's classification of the severity of attacks into the invention of Yavatkar in order minimize the load on the computer network. Displaying attack information would help the network manager prioritize the severity of the attacks so that it spend less time countering lesser threats and more time countering severe threats (col. 2, lines 47-53).

(10) Response to Argument

The examiner summarized the various points raised by the appellant and addressed replies individually.

As per appellants arguments filed on March 14, 2007, the appellant argues:

(A) Argument (claims 1, 7, 8, and 10-14): Yavatkar fails to disclose sending queries to data collectors... that... collect statistical information on network packets sent over the network, the queries to request the statistical information from at least some of the data collectors... and processing the statistical information to determine the source of suspicious network traffic sent to the data center (refer to brief pages 9-15).

Response to (A)

Yavatkar teaches analyzing traffic on a network by monitoring network traffic and, when a particular network condition (for example, a network attack) is detected, gathering information about the traffic on the network by launching an agent and having the agent iteratively identify which of the links on the node on which the agent operates accepts a type or class of traffic, traverse the identified link to the node across the link, and repeat the process. Yavatkar teaches:

> In an exemplary embodiment of the present invention, a watchdog agent monitors the node on which it operates for traffic having characteristics of a network attack. A watchdog agent may also monitor for and detect a network attack at a device other than the device on which it operates. On detecting an attack the **watchdog agent launches one or more bloodhound agents** to trace the attack traffic. The watchdog agent launches various types of bloodhound agents based on the type of attack detected; each bloodhound agent is designed to trace traffic from one type of attack. In an exemplary embodiment a bloodhound agent moves across the network, tracing the path or paths taken by attack traffic. To trace attack traffic, the bloodhound agent follows an iterative process of finding the port for the link on the node on which it operates which is accepting attack traffic, attempting to traverse that link (i.e., to move to the node on the other side of the link) to a new node, and, once at the new node, again finding the port and link which are accepting attack traffic. In such a manner the path or paths, or a portion of the path or paths, of attack traffic between **the source of the attack traffic** and the target node may be found. After gathering such information a **bloodhound agent reports to the watchdog agent**, which, in turn, may report to a human operator or,

> possibly, attempt to halt the attack. A target node is a node to which attack traffic is directed or which attack traffic affects.
> (Refer to Yavatkar at col. 13, lines 44-53, emphasis added).

Yavatkar further teaches:

> In step 404 watchdog agent 114 launches bloodhound agent 116 and waits for a response from bloodhound agent 116.
> (Refer to Yavatkar at col. 19, lines 64-66, emphasis added).

The appellant is reminded that the claims must be given their broadest reasonable interpretation. The claim language merely recites sending queries to data collectors...to request statistical information and does not specify the type of query. Yavatkar teaches wherein on detecting an attack the watchdog agent launches various types of bloodhound agents based on the type of attack detected. Examiner is equating the launching of the various types of bloodhound agents to launching various types of queries to each bloodhound agent upon its creation based on the type of attack detected. After launching the bloodhound agents the watchdog agents wait for a response *(response to what? response to the launching of the bloodhound agents equated to the claimed query)*. Each bloodhound agents is designed to trace traffics from one type of attack.

Yavatkar further teaches:

> A watchdog agent may assume a network attack exists if network congestion is detected. To detect network congestion a watchdog agent monitors the number of packets, which were to be received at the node on which the watchdog agent operates but which have been lost. The watchdog agent detects **lost incoming packets** by monitoring the TCP/IP stack, maintained in the operating system. If the number of incoming lost packets rises above a certain level the watchdog agent concludes a congestion condition exists...
>
> ...the watchdog agent launches one or more bloodhound agents to trace the attack traffic to its **source** and analyze the paths taken by the attack traffic. Each bloodhound agent is

> designed to trace traffic from one attack. The watchdog agent launches different types of bloodhound agents based on the type of attack detected. If a TCP/SYN attack is detected the watchdog agent launches a bloodhound agent designed to trace such an attack; such an agent traces TCP/SYN traffic for the targeted device. If another type of attack, such as a ping of death attack, is detected, a bloodhound agent tracing traffic characteristic of such an attack is launched. If appropriate, the watchdog agent is provided with information necessary to trace the attack traffic, such as the IP address of the node being targeted. If an attack is assumed based on network congestion or node unreachability, multiple agents, each tracing traffic based on one type of attack, are launched. In such a case only one type of bloodhound agent may successfully trace the attack, and the bloodhound may not be provided with the identity of the device being attacked.
> (Refer to Yavatkar at col. 15, line 63 – col. 16, line 45).

The information gathered on the attack traffic (packets in the network) by the bloodhound agents is equated to the statistical information because the claim language merely recites statistical information on packets in a network and does not specify the type of statistical information that is collected. After gathering information (statistical information) a bloodhound agent reports to the watchdog agent automatically without having to wait for the watchdog agent to request the information because the request has been established upon the creation of the bloodhound agent and therefore a second request is not needed. The gathered information are processed in order to determine the source of the attack and to diagnose and ultimately try to eliminate the attack. Therefore, Yavatkar creation of the bloodhound agents and gathering of the information by the agents meets the scope of the claimed limitations.

(B) Argument (claim 2): Yavatkar fails to disclose sending queries to the data collectors for the statistical information based on victim destination address (refer to brief pages 15-16).

Response to (B)

Yavatkar teaches:

> If the source of the attack traffic messages can be identified (by, for example, its IP address) the source can be shut down or disabled. For example, the Internet provider allowing the source device access to the Internet may be notified and may terminate the source device's Internet access. However, through the use of IP spoofing the source of the attack may be obscured. Using IP spoofing the TCP/IP packets constituting the attack traffic indicate a source which is not the actual source device--the sender of the attack traffic inserts a false "return address."
>
> In a network having multiple gateways to other networks, if the particular gateway allowing attack traffic onto the network can be identified, the attack can be halted. Either the gateway can be shut down or the appropriate filter can be installed on the gateway. (Refer to Yavatkar at col. 13, lines 44-65).

The bloodhound agents respond to the watchdog agents with the gathered information. The gathered information contains data on the source of the attack and specifically the gateways or nodes (victim) that are allowing the attack traffic. Yavatkar further teaches where appropriate action may be taken, such as installing firewall entries at the appropriate devices to block such traffic. Therefore Yavatkar is very much concerned with gathered information based on the gateways destination address (victim destination address) in order to be able to install appropriate firewalls to block the attack traffic and as such meets the scope of the claimed limitation.

(C) Argument (claim 3): The examiner has not shown that Yavatkar inherently possess the clamed statistical information (refer to brief page 16).

Response to (C)

The information gathered on the attack traffic (packets in the network) by the bloodhound agents is equated to the statistical information because the claim language

merely recites statistical information on packets in a network and does not specify the type of statistical information that is collected. After gathering information (statistical information) a bloodhound agent reports to the watchdog agent automatically without having to wait for the watchdog agent to request the information because the request has been established upon the creation of the bloodhound agent and therefore a second request is not needed. The gathered information are processed in order to determine the source of the attack and to diagnose and ultimately try to eliminate the attack. Therefore, Yavatkar creation of the bloodhound agents and gathering of the information by the agents meets the scope of the claimed limitations.

(D) Argument (claims 4 and 5): Yavatkar fails to disclose determining is performed by a control center that receives the statistical information from the data collectors and includes sending data to/from a gateway device that is associated with the victim data center (refer to brief pages 16-17).

Response to (D)

Yavatkar teaches:

> After a response from the bloodhound agent the watchdog agent transitions to the respond mode. In the respond mode the watchdog agent may attempt to halt the attack. For example the watchdog agent may launch an agent which alters routing tables to prohibit traffic from a given source from entering the network, or may perform such an operation itself The watchdog agent may launch an agent which functions as a firewall; such an agent moves to the point in the network which is the ingress point for attack traffic. The watchdog agent may install several intermediate filters in the network which prevent attack traffic from being forwarded. The watchdog agent may report findings (e.g., the source of the attack; the path or paths taken by attack traffic) to a network administrator. In an exemplary embodiment the watchdog agent communicates with network administrators via a management console application; alternate embodiments may use other methods. The network administrator may use the findings to cure the

problem. After attempting to halt the attack or contact an administrator the watchdog agent transitions to the monitoring mode.
(Refer to Yavatkar at col. 17, lines 11-31).

A watchdog agent may exist in monitoring mode, where it monitors for network attacks; alert mode, where it creates bloodhound agents and waits for bloodhound agents to report; and respond mode, where it reports to a network administrator with information about the attack and/or takes measures to block or stop the attack. Watchdog agent reacts to input from a human operator to enter the different modes. The watchdog agent communicates with network administrators via a management console application; alternate embodiments may use other methods. The network administrator may use the findings to cure the problem. Therefore Yavatkar meets the scope of the clamed limitation.

(E) Argument (claim 6): Yavatkar fails to disclose that the queries and the statistical information are sent over a redundant network that does not carry the packet traffic to deliver collected statistical information to a central control in response to the queries sent from the central center (refer to brief pages 17-18).

Response to (E)

The watchdog agent may report findings (e.g., the source of the attack; the path or paths taken by attack traffic) to a network administrator. In an exemplary embodiment the watchdog agent communicates with network administrators via a management console application; alternate embodiments may use other methods. The network administrator may use the findings to cure the problem. After attempting to halt the

attack or contact an administrator the watchdog agent transitions to the monitoring mode. Therefore, Yavatkar's meets the scope of the claimed limitation.

(F) Argument (claim 9): Yavatkar fails to disclose if a source of the attack is behind a gateway, the control center issues a request to the gateway that the attacking system is behind to prevent the attacking traffic...from reaching the network (refer to brief pages 18-19).

Response to (F)

The bloodhound agent provides to the watchdog agent a report indicating the path or paths (or a portion of the path or paths) taken by the attack traffic and, possibly, the source of the attack traffic. The source may be indicated as a gateway allowing access to other networks; in such a case the indicated source is not the originating source of the attack. If the particular gateway allowing attack traffic onto the network can be identified, the attack can be halted. The network administrator may use the findings to cure the problem. Yavatkar further teaches where appropriate action may be taken, such as installing firewall entries at the appropriate devices to block such traffic or issue a request to the gateway to shut down in order to prevent the attacking traffic from the reaching the network. Therefore, Yavatkar meets the scope of the claimed limitation.

(G) Argument (claim 15): Yavatkar does not teach receiving a notification that the victim is under attack (refer to brief page 19.

Response to (G)

Yavatkar teaches:

> In an exemplary embodiment a watchdog agent may detect a network attack at a device other than the device on which it operates. A watchdog agent may monitor for an attack on a remote device if, for example, the remote device cannot support a watchdog agent or if a type of attack may occur which cannot be detected at the device being attacked. Each watchdog agent may be assigned a set of devices to monitor. The watchdog agent periodically attempts to make a TCP connection to each assigned remote device. If a connection cannot be made, the watchdog agent presumes a TCP attack is occurring with the remote device as a target. The watchdog agent may use a service to monitor incoming and/or outgoing packets at the remote device, and interpret these packets in the same manner as packets sent from and received at the device on which it operates. A watchdog agent may also periodically determine reachability to an assigned device, using, for instance, a ping message. That other devices in a network are not reachable may indicate an attack on those devices. A watchdog agent uses services to access capabilities such as making TCP connections and ping transmission.
> (Refer to Yavatkar at col. 15, lines 52-62).

Yavatkar teaches that the watchdog agent periodically attempts to make a TCP connection to each assigned remote device. If a connection cannot be made, the watchdog agent presumes a TCP attack is occurring with the remote device as a target. Yavatkar further teaches wherein a watchdog agent may also periodically determine reachability to an assigned device, using, for instance, a ping message. That other devices in a network are not reachable may indicate an attack on those devices. The claims merely recite notification and do not specify the type of notification and as such are broadly interpreted. If the watchdog agent can not make TCP connection to a network device or determines that a network device to be unreachable it is presumed to be under attack. The network device notifies the watchdog agent of an attack when it does not establish the TCP connection or it is unreachable. Therefore, Yavatkar meets the cope of the claimed limitation

(H) Argument (claims 16): Yavatkar fails to disclose communicating statistical information from the control center to/from a gateway device that is disposed with the victim data center (refer to brief pages 19).

Response to (H)

Yavatkar teaches:

> After a response from the bloodhound agent the watchdog agent transitions to the respond mode. In the respond mode the watchdog agent may attempt to halt the attack. For example the watchdog agent may launch an agent which alters routing tables to prohibit traffic from a given source from entering the network, or may perform such an operation itself The watchdog agent may launch an agent which functions as a firewall; such an agent moves to the point in the network which is the ingress point for attack traffic. The watchdog agent may install several intermediate filters in the network which prevent attack traffic from being forwarded. The watchdog agent may report findings (e.g., the source of the attack; the path or paths taken by attack traffic) to a network administrator. In an exemplary embodiment the watchdog agent communicates with network administrators via a management console application; alternate embodiments may use other methods. The network administrator may use the findings to cure the problem. After attempting to halt the attack or contact an administrator the watchdog agent transitions to the monitoring mode.
> (Refer to Yavatkar at col. 17, lines 11-31).

A watchdog agent may exist in monitoring mode, where it monitors for network attacks; alert mode, where it creates bloodhound agents and waits for bloodhound agents to report; and respond mode, where it reports to a network administrator with information about the attack and/or takes measures to block or stop the attack. Watchdog agent reacts to input from a human operator to enter the different modes. The watchdog agent communicates with network administrators via a management console application; alternate embodiments may use other methods. The network administrator may use the findings to cure the problem. Therefore Yavatkar meets the scope of the clamed limitation.

(I) Argument (claim 17): Yavatkar fails to disclose the control center issues a request to the gateway to block the attacking traffic (refer to brief pages 20).

Response to (I)

The bloodhound agent provides to the watchdog agent a report indicating the path or paths (or a portion of the path or paths) taken by the attack traffic and, possibly, the source of the attack traffic. The source may be indicated as a gateway allowing access to other networks; in such a case the indicated source is not the originating source of the attack. If the particular gateway allowing attack traffic onto the network can be identified, the attack can be halted. The network administrator may use the findings to cure the problem. Yavatkar further teaches where appropriate action may be taken, such as installing firewall entries at the appropriate devices to block such traffic or issue a request to the gateway to shut down in order to prevent the attacking traffic from the reaching the network. Therefore, Yavatkar meets the scope of the claimed limitation.

(J) Argument (claims 20, 21 and 26-28): Yavatkar fails to disclose sending queries to data collectors... that... collect statistical information on network packets sent over the network, the queries to request the statistical information from at least some of the data collectors... and processing the statistical information to determine the source of suspicious network traffic sent to the data center (refer to brief pages 20).

Response to (J)

Yavatkar teaches analyzing traffic on a network by monitoring network traffic and, when a particular network condition (for example, a network attack) is detected, gathering information about the traffic on the network by launching an agent and having the agent iteratively identify which of the links on the node on which the agent operates accepts a type or class of traffic, traverse the identified link to the node across the link, and repeat the process. Yavatkar teaches:

> In an exemplary embodiment of the present invention, a watchdog agent monitors the node on which it operates for traffic having characteristics of a network attack. A watchdog agent may also monitor for and detect a network attack at a device other than the device on which it operates. On detecting an attack the **watchdog agent launches one or more bloodhound agents** to trace the attack traffic. The watchdog agent launches various types of bloodhound agents based on the type of attack detected; each bloodhound agent is designed to trace traffic from one type of attack. In an exemplary embodiment a bloodhound agent moves across the network, tracing the path or paths taken by attack traffic. To trace attack traffic, the bloodhound agent follows an iterative process of finding the port for the link on the node on which it operates which is accepting attack traffic, attempting to traverse that link (i.e., to move to the node on the other side of the link) to a new node, and, once at the new node, again finding the port and link which are accepting attack traffic. In such a manner the path or paths, or a portion of the path or paths, of attack traffic between **the source of the attack traffic** and the target node may be found. After gathering such information a **bloodhound agent reports to the watchdog agent**, which, in turn, may report to a human operator or, possibly, attempt to halt the attack. A target node is a node to which attack traffic is directed or which attack traffic affects.
> (Refer to Yavatkar at col. 13, lines 44-53, emphasis added).

Yavatkar further teaches:

> In step 404 watchdog agent 114 launches bloodhound agent 116 and waits for a response from bloodhound agent 116.
> (Refer to Yavatkar at col. 19, lines 64-66, emphasis added).

The appellant is reminded that the claims must be given their broadest reasonable interpretation. The claim language merely recites sending queries to data collectors...to request statistical information and does not specify the type of query.

Yavatkar teaches wherein on detecting an attack the watchdog agent launches various types of bloodhound agents based on the type of attack detected. Examiner is equating the launching of the various types of bloodhound agents to launching various types of queries to each bloodhound agent upon its creation based on the type of attack detected. After launching the bloodhound agents the watchdog agents wait for a response *(response to what? response to the launching of the bloodhound agents equated to the claimed query)*. Each bloodhound agents is designed to trace traffics from one type of attack.

Yavatkar further teaches:

> A watchdog agent may assume a network attack exists if network congestion is detected. To detect network congestion a watchdog agent monitors the number of packets, which were to be received at the node on which the watchdog agent operates but which have been lost. The watchdog agent detects **lost incoming packets** by monitoring the TCP/IP stack, maintained in the operating system. If the number of incoming lost packets rises above a certain level the watchdog agent concludes a congestion condition exists…
>
> …the watchdog agent launches one or more bloodhound agents to trace the attack traffic to its **source** and analyze the paths taken by the attack traffic. Each bloodhound agent is designed to trace traffic from one attack. The watchdog agent launches different types of bloodhound agents based on the type of attack detected. If a TCP/SYN attack is detected the watchdog agent launches a bloodhound agent designed to trace such an attack; such an agent traces TCP/SYN traffic for the targeted device. If another type of attack, such as a ping of death attack, is detected, a bloodhound agent tracing traffic characteristic of such an attack is launched. If appropriate, the watchdog agent is provided with information necessary to trace the attack traffic, such as the IP address of the node being targeted. If an attack is assumed based on network congestion or node unreachability, multiple agents, each tracing traffic based on one type of attack, are launched. In such a case only one type of bloodhound agent may successfully trace the attack, and the bloodhound may not be provided with the identity of the device being attacked.
> (Refer to Yavatkar at col. 15, line 63 – col. 16, line 45).

The information gathered on the attack traffic (packets in the network) by the bloodhound agents is equated to the statistical information because the claim language

merely recites statistical information on packets in a network and does not specify the type of statistical information that is collected. After gathering information (statistical information) a bloodhound agent reports to the watchdog agent automatically without having to wait for the watchdog agent to request the information because the request has been established upon the creation of the bloodhound agent and therefore a second request is not needed. The gathered information are processed in order to determine the source of the attack and to diagnose and ultimately try to eliminate the attack. Therefore, Yavatkar creation of the bloodhound agents and gathering of the information by the agents meets the scope of the claimed limitations.

(K) Argument (claims 22): Yavatkar fails to disclose that the control center further comprises instructions to determine a source of the attack on the victim data center by analyzing collected statistical information from the data collectors(refer to brief pages 21).

Response to (K)

Yavatkar teaches:

> After a response from the bloodhound agent the watchdog agent transitions to the respond mode. In the respond mode the watchdog agent may attempt to halt the attack. For example the watchdog agent may launch an agent which alters routing tables to prohibit traffic from a given source from entering the network, or may perform such an operation itself The watchdog agent may launch an agent which functions as a firewall; such an agent moves to the point in the network which is the ingress point for attack traffic. The watchdog agent may install several intermediate filters in the network which prevent attack traffic from being forwarded. The watchdog agent may report findings (e.g., the source of the attack; the path or paths taken by attack traffic) to a network administrator. In an exemplary embodiment the watchdog agent communicates with network administrators via a management console application; alternate embodiments may use other methods. The network administrator may use the findings to cure the

problem. After attempting to halt the attack or contact an administrator the watchdog agent transitions to the monitoring mode.
(Refer to Yavatkar at col. 17, lines 11-31).

A watchdog agent may exist in monitoring mode, where it monitors for network attacks; alert mode, where it creates bloodhound agents and waits for bloodhound agents to report; and respond mode, where it reports to a network administrator with information about the attack and/or takes measures to block or stop the attack. Watchdog agent reacts to input from a human operator to enter the different modes. The watchdog agent communicates with network administrators via a management console application; alternate embodiments may use other methods. The network administrator may use the findings to cure the problem and identify the source of the attack. Therefore Yavatkar meets the scope of the clamed limitation.

(L) Argument (claim 23): Yavatkar fails to disclose the control center issues and gateway device associated with the victim data center exchange data including statistical information to thwart the attack (refer to brief pages 21).

Response to (L)

The bloodhound agent provides to the watchdog agent a report indicating the path or paths (or a portion of the path or paths) taken by the attack traffic and, possibly, the source of the attack traffic. The source may be indicated as a gateway allowing access to other networks; in such a case the indicated source is not the originating source of the attack. If the particular gateway allowing attack traffic onto the network can be identified, the attack can be halted. The network administrator may use the

findings to cure the problem. Yavatkar further teaches where appropriate action may be taken, such as installing firewall entries at the appropriate devices to block such traffic or issue a request to the gateway to shut down in order to prevent the attacking traffic from the reaching the network. Therefore, Yavatkar meets the scope of the claimed limitation.

(M) Argument (claim 24): Yavatkar fails to disclose that the queries and the statistical information are sent over a redundant network that does not carry the packet traffic to deliver collected statistical information to a central control in response to the queries sent from the central center (refer to brief pages 21).

Response to (M)

The watchdog agent may report findings (e.g., the source of the attack; the path or paths taken by attack traffic) to a network administrator. In an exemplary embodiment the watchdog agent communicates with network administrators via a management console application; alternate embodiments may use other methods. The network administrator may use the findings to cure the problem. After attempting to halt the attack or contact an administrator the watchdog agent transitions to the monitoring mode. Therefore, Yavatkar's meets the scope of the claimed limitation.

(N) Argument (claim 25): appellant argues that claim 25 is allowable for analogous reasons as given in claim 9 (refer to brief pages 21).

Response to (N)

Refer to Argument (F) with reference to claim 9 for a full response.

(O) Argument (claims 29 and 32): Yavatkar fails to disclose sending queries to data collectors... that... collect statistical information on network packets sent over the network, the queries to request the statistical information from at least some of the data collectors... and processing the statistical information to determine the source of suspicious network traffic sent to the data center (refer to brief pages 21-22).

Response to (O)

Yavatkar teaches analyzing traffic on a network by monitoring network traffic and, when a particular network condition (for example, a network attack) is detected, gathering information about the traffic on the network by launching an agent and having the agent iteratively identify which of the links on the node on which the agent operates accepts a type or class of traffic, traverse the identified link to the node across the link, and repeat the process. Yavatkar teaches:

> In an exemplary embodiment of the present invention, a watchdog agent monitors the node on which it operates for traffic having characteristics of a network attack. A watchdog agent may also monitor for and detect a network attack at a device other than the device on which it operates. On detecting an attack the **watchdog agent launches one or more bloodhound agents** to trace the attack traffic. The watchdog agent launches various types of bloodhound agents based on the type of attack detected; each bloodhound agent is designed to trace traffic from one type of attack. In an exemplary embodiment a bloodhound agent moves across the network, tracing the path or paths taken by attack traffic. To trace attack traffic, the bloodhound agent follows an iterative process of finding the port for the link on the node on which it operates which is accepting attack traffic, attempting to traverse that link (i.e., to move to the node on the other side of the link) to a new node, and, once at the new node, again finding the port and link which are accepting attack traffic. In such a manner the path or paths, or a portion of the path or paths, of attack traffic between **the source of the attack traffic** and the target node may be found. After gathering such information a **bloodhound agent reports to the watchdog agent**, which, in turn, may report to a human operator or,

> possibly, attempt to halt the attack. A target node is a node to which attack traffic is directed or which attack traffic affects.
> (Refer to Yavatkar at col. 13, lines 44-53, emphasis added).

Yavatkar further teaches:

> In step 404 watchdog agent 114 launches bloodhound agent 116 and waits for a response from bloodhound agent 116.
> (Refer to Yavatkar at col. 19, lines 64-66, emphasis added).

The appellant is reminded that the claims must be given their broadest reasonable interpretation. The claim language merely recites sending queries to data collectors...to request statistical information and does not specify the type of query. Yavatkar teaches wherein on detecting an attack the watchdog agent launches various types of bloodhound agents based on the type of attack detected. Examiner is equating the launching of the various types of bloodhound agents to launching various types of queries to each bloodhound agent upon its creation based on the type of attack detected. After launching the bloodhound agents the watchdog agents wait for a response *(response to what? response to the launching of the bloodhound agents equated to the claimed query)*. Each bloodhound agents is designed to trace traffics from one type of attack.

Yavatkar further teaches:

> A watchdog agent may assume a network attack exists if network congestion is detected. To detect network congestion a watchdog agent monitors the number of packets, which were to be received at the node on which the watchdog agent operates but which have been lost. The watchdog agent detects **lost incoming packets** by monitoring the TCP/IP stack, maintained in the operating system. If the number of incoming lost packets rises above a certain level the watchdog agent concludes a congestion condition exists...
>
> ...the watchdog agent launches one or more bloodhound agents to trace the attack traffic to its **source** and analyze the paths taken by the attack traffic. Each bloodhound agent is designed to trace traffic from one attack. The watchdog agent launches different types of

> bloodhound agents based on the type of attack detected. If a TCP/SYN attack is detected the watchdog agent launches a bloodhound agent designed to trace such an attack; such an agent traces TCP/SYN traffic for the targeted device. If another type of attack, such as a ping of death attack, is detected, a bloodhound agent tracing traffic characteristic of such an attack is launched. If appropriate, the watchdog agent is provided with information necessary to trace the attack traffic, such as the IP address of the node being targeted. If an attack is assumed based on network congestion or node unreachability, multiple agents, each tracing traffic based on one type of attack, are launched. In such a case only one type of bloodhound agent may successfully trace the attack, and the bloodhound may not be provided with the identity of the device being attacked.
> (Refer to Yavatkar at col. 15, line 63 – col. 16, line 45).

The information gathered on the attack traffic (packets in the network) by the bloodhound agents is equated to the statistical information because the claim language merely recites statistical information on packets in a network and does not specify the type of statistical information that is collected. After gathering information (statistical information) a bloodhound agent reports to the watchdog agent automatically without having to wait for the watchdog agent to request the information because the request has been established upon the creation of the bloodhound agent and therefore a second request is not needed. The gathered information are processed in order to determine the source of the attack and to diagnose and ultimately try to eliminate the attack. Therefore, Yavatkar creation of the bloodhound agents and gathering of the information by the agents meets the scope of the claimed limitations.

(P) Argument (claim 30): appellant argues that claim 30 is allowable for analogous reasons as given in claim 16 (refer to brief pages 22).

Response to (P)

Refer to Argument (H) with reference to claim 16 for a full response.

(Q) Argument (claim 31): appellant argues that claim 31 is allowable for analogous reasons as given in claim 9 (refer to brief pages 22).

Response to (Q)

Refer to Argument (F) with reference to claim 9 for a full response.

(R) Argument (claims 13 and 14): appellant argues that Hill does not cure the deficiencies of Yavatkar and further that the teaching of Hill are directed to attack simulation not to an actual attack.

Response to (R)

These limitations are not found in the claims. Claimed subject matter not the specification is the measure of the invention. Disclosure contained in the specification cannot be read into the claims for the purpose of avoiding prior art. In re Sporck, 55 CCPA 743, 386 F .2d. Hill teaches a system and method for adaptively responding to computer network security attacks. Hill further teaches classifying attacks based on the severity of the attack on the network (Fig. 3, col. 2; lines 53-60; col. 6, lines 9-22). The claims merely recite attack and do not specify that the attack be real attacks or attacks that are not simulated. Therefore, Hill's simulated attacks meet the scope of the claimed limitation and render the claims obvious.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Shawki Ismail

Conferees:

Lynne Browne
Appeal specialist TC 2100

Saleh Najjar
SPE AU 2155